AMENDMENT TO THE CLAIMS

This listing of claims will replace all prior versions, and listings, of claims in the application:

Listing of Claims:

1. (currently amended) In a node operative within a network of a plurality of nodes, a method for performing cryptographic-related functions, comprising:

executing an application program in a user space at the node;

receiving an input requiring cryptographic-related processing;

generating a message in the node via the application program based on the input, the message ~~representing~~ being the same as one of a predefined set of messages stored in the node and being processed ~~for processing~~ by one of a plurality of cryptographic processing components located in a kernel space within the node, each one of said messages being associated with a respective one of said cryptographic-related functions;

transmitting the message to one of a socket handler and a call handler in kernel space at the node to obtain a transmitted message;

forwarding the transmitted message to a request handler at the node which generates a function call to the cryptographic processing component appropriate for the transmitted message; and

performing the cryptographic-related processing by the cryptographic processing component appropriate for the transmitted message.

2. (previously presented) The method of claim 1, wherein the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate in the node; or certificate age checking.

3. (previously presented) The method of claim 1,wherein the transmitting includes:

generating a user datagram protocol (UDP) message containing an identifier associated with a predetermined cryptographic-related function and transmitting the UDP message via a UDP socket to the socket handler.

4. (previously presented) The method of claim 1, further comprising:

generating an output message via the application program, the output message requiring cryptographic-related processing;

transmitting, based on the required cryptographic-related processing, one of the predefined set of messages to the cryptographic processing component;

performing the cryptographic-related processing; and

outputting the processed message.

5. (currently amended) A computer-readable medium <u>in a node operating within a network of nodes, the node including a processor, the medium</u> having stored thereon a plurality of sequences of instructions that may be invoked by a plurality of predefined

messages, said instructions including sequences of instructions which, when executed by [[a]] the processor in a user space, cause said processor to perform a method comprising:

receiving an input from the network representing one of the predefined messages;

generating ~~transmitting~~, within the node and based on the input, a function call representing a request for cryptographic-related processing, and transmitting within the node said function call to a cryptographic processing module ~~executed by the processor~~; and

performing the cryptographic-related processing in a kernel space;

wherein at least the receiving, the transmitting and the performing are implemented by public key authentication infrastructure (PKAI) comprising:

user space components including a user application program, a PKAI control daemon, a certificate database, a PKAI operations daemon and a PKAI remote server daemon; and

kernel space components including a PKAI socket handler, a PKAI call handler and a PKAI request handler;

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components communicate with other of the kernel space components; and

wherein other certain of the user space components communicate with other certain of the kernel space components.

6. (previously presented) The computer-readable medium of claim 5, wherein the performing the cryptographic-related processing includes at least one of:

verifying or generating a digital signature; encrypting or decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; or certificate age checking.

7. (canceled)

8. (original) The computer-readable medium of claim 5, wherein the input represents a digitally signed network control message requiring verification.

9. (currently amended) A cryptographic module in a node operative within a network of nodes, said module comprising:

a memory configured to store a plurality of cryptographic processing programs in user space on a computer-readable medium, each program being invoked via one of a plurality of predefined messages; and

a processor configured to:

receive an input from the network requiring cryptographic-related processing,

generate within the node one of the predefined messages based on the input,

transmit within the node the message to the memory to invoke a first one of the cryptographic processing programs, and

perform, in kernel space, the cryptographic-related processing;

wherein the module receives, generates, transmits and performs through infrastructure comprising:

user space components including a user application program, a control daemon, a certificate database, an operations daemon and a remote server daemon; and

kernel space components including a socket handler, a call handler and a request handler;

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components communicate with other of the kernel space components; and

wherein other certain of the user space components communicate with other certain of the kernel space components.

10. (previously presented) The cryptographic module of claim 9, wherein when performing the cryptographic-related processing, the processor is configured to perform at least one of:

verifying or generating a digital signature; encrypting data; decrypting data; retrieving a digital certificate or certificate revocation list; verifying a certificate's hierarchy; self-signed certificate processing; retrieving, verifying and storing a digital certificate; or certificate age checking.

11. (original) The cryptographic module of claim 9, wherein when transmitting the message, the processor is further configured to:

transmit a function call to the first cryptographic processing program.

12. (original) The cryptographic module of claim 9, wherein the processor is further configured to:

transmit the result of the cryptographic-related processing to an application program.

13. (canceled)

14. (currently amended) A method of performing cryptographic-related functions in a node coupled to other nodes in a network, the node including an application program executed in user space for handling communications with the other nodes, the method comprising:

receiving in said node from one of said other nodes an input requiring a cryptographic-related operation;

generating in said node a predefined message based on the input, the message representing one of a plurality of predefined messages usable by a cryptographic processing program executed by one of a plurality of cryptographic processing components in kernel space, each one of said messages being associated with a respective one of said cryptographic-related functions;

transmitting in said node the predefined message to a socket handler in kernel space or a call handler in kernel space to obtain a transmitted message;

forwarding the transmitted message to a request handler within the node which generates a function call to the cryptographic processing component appropriate for the transmitted message; and

performing in said node, via the cryptographic processing program, the required cryptographic-related operation.

15. (original) The method of claim 14, further comprising:

returning the result of the performing to the application program.

16. (previously presented) The method of claim 14, wherein the predefined message includes at least one of:

a request for digital signature generation, a request for digital signature verification, a request for data encryption, a request for data decryption, a request for retrieval of a digital certificate, a request for retrieval of a certificate revocation list, a request for verification of a certificate's hierarchy, a request for self-signed certificate processing, or a request for certificate age checking.

17. (previously presented) The method of claim 16, wherein the request for digital signature generation includes a request for at least one of RSA signature generation, secret keyed MD5 signature generation, elliptic curve signature generation or digital signature standard signature generation.

18. (previously presented) The method of claim 16, wherein the request for digital signature verification includes a request for at least one of RSA signature verification, secret keyed MD5 signature verification, elliptic curve signature verification or digital signature standard signature verification.

19. (previously presented) The method of claim 16, wherein the request for data encryption includes a request for at least one of RSA based encryption or elliptic curve based encryption.

20. (previously presented) The method of claim 16, wherein the request for data decryption includes a request for at least one of RSA based decryption or elliptic curve based decryption.

21. (original) The method of claim 14, wherein the performing includes:

accessing a remote server via the network to retrieve cryptographic-related information.

22. (currently amended) In a node operating within a network, a [[A]] computer-readable medium that stores instructions in user space executable in kernel space by at least one processor in the node ~~in kernel space~~ to perform a method for providing cryptographic-related functions, the method comprising:

receiving, responsive to input to the node from another node in the network, in the at least one processor a first function call from a predefined list of function calls, the predefined list of function calls representing available cryptographic-related functions executable by the at least one processor;

generating in the at least one processor in the node a request message based on the first function call, the request message representing a request for processing by a cryptographic processing module ~~executed by the at least one processor~~;

transmitting in the node ~~at least one processor~~ the request message to the cryptographic processing module; and

performing in the at least one processor the cryptographic-related function;

wherein the receiving, the generating the transmitting and the performing are implemented by:

user space components including a user application program, a control daemon, a certificate database, a operations daemon and a remote server daemon; and

kernel space components including a socket handler, a call handler and a request handler;

wherein certain of the user space components communicate with other of the user space components and certain of the kernel space components communicate with other of the kernel space components; and

wherein other certain of the user space components communicate with other certain of the kernel space components.

23. (canceled)

REMARKS

This Amendment is responsive to the Office Action[1] of February 12, 2008. Claims 1, 5, 9, 14 and 22 are in independent form and are currently amended. Claims 7, 13 and 23 were previously canceled without prejudice or disclaimer. Thus, claims 1-6, 8-12 and 14-22 remain pending. No new matter is added. Support for the amendments made herein can be found in the application as originally filed. For example, see, at least, page 12, line 21 through page 13, line 19; page 14, lines 3-5 and 10-12; and Appendix A.

Claims 1-4, 9-12, 14-18, and 21-22 are rejected under 35 U.S.C. § 103(a) as being un-patentable over Minear et al. (U.S. Patent No. 5,983,350; hereinafter "Minear") and further in view of Mason et al. (U.S. Patent No. 5,668,998; hereinafter "Mason"). Claims 5-6, 8 and 19-20 are rejected under 35 U.S.C. § 103(a) as being un-patentable over Minear and Mason and further in view of Gennaro (U.S, Patent No. 5,937,066; hereinafter "Gennaro").

The Office Action (pg 2) advises that Applicants' previous arguments filed November 15, 2007 rebutting Minear and Mason were persuasive wherefore "the rejection has been withdrawn" and "a new ground of rejection is made in view of Minear and Gennaro." Despite this admitted persuasiveness of Applicants' arguments, Minear and Mason, with and without Gennaro, are again relied-upon to reject the pending claims, as noted above.

[1] The Office Action may contain a number of statements characterizing the cited references and/or the claims which Applicants may not expressly identify herein. Regardless of whether or not any such statement is identified herein, Applicants do not automatically subscribe to, or acquiesce in, any such statement.